UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/720,211 | 11/25/2003 | Hidekazu Tanno | Q78595 | 4996 |

23373 7590 10/30/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

| EXAMINER | |
|---|---|
| DAO, THUY CHAN | |
| **ART UNIT** | **PAPER NUMBER** |
| 2192 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 10/30/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/720,211 | TANNO ET AL. | |
| | Examiner | Art Unit | |
| | Thuy Dao | 2192 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,3,5,6,9-11 and 13-19* is/are pending in the application.

4a) Of the above claim(s) *2,4,7,8 and 12* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5,6,9-11 and 13-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is responsive to the amendment filed on July 8, 2008.

2. Claims 1, 3, 5-6, 9-11, and 13-19 have been examined.

### Response to Amendments

3. In the instant amendment, claims 1, 3, 5-6, 9-11, and 13 have been amended; claims 2, 4, 7-8, and 12 have been canceled.

### Response to Arguments

4. Applicants' arguments have been considered but are moot in view of the new ground(s) of rejection.

### Claim Rejections – 35 USC §101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 10, 11, and 13 are rejected because the claimed invention is directed to non-statutory subject matter: independent claims 1 and 11 direct to "A detection program ...", which may comprise only software components as claimed.

Claims 10 and 11 amount to Functional Descriptive Material: "Data Structures" representing descriptive material per se or "Computer Programs" representing computer listings per se.

Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data

structure's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory.

Similarly, computer programs claimed as computer listings per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions. See MPEP 2106.

Dependent claim 13 does not cure the deficiencies as noted above, thus, also amount to Functional Descriptive Material: "Data Structures" representing descriptive material per se or "Computer Programs" representing computer listings per se.

Under the principles of compact prosecution, claims 10, 11, and 13 have been examined as the Examiner anticipates the claims will be amended to obviate these 35 USC § 101 issues. For example, - -A detection program, embedded in a computer-readable storage medium, for omission-in-software-property-management... - - as disclosed in the specification, page 28: 28 – page 29: 9.

**Claim Rejections – 35 USC §102**

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1, 3, 5-6, 9-11, and 13-19 are rejected under 35 U.S.C. 102(b) as being anticipated by "SafePatch Version 0.9 User Manual", March 1999 (art made of record, hereafter "SafePatch").

**Claim 1:**

SafePatch discloses *a detection method of omission-in-software-property-management using a network for detecting a computer omitted from a software-property management which manages, for each computer, basic information thereof and installed software, and fix-patch application status, the method comprising the steps of:*

*performing a first step wherein a network-connected-computer list* (e.g., Figure in page 31, list of alive remote systems/hosts after successfully testing their communications with Patch Server, page 30, section 4.3)

*which holds, for all computers connected to a given network, information for identifying each computer* (e.g., page 2, section 1.1.1.2 Evaluating Remote Systems; page 34, host specification with OS type, name, version, and hardware type), *and*

*a software-property management list* (e.g., SafePatch overview, Figure in page 1 and pp. 17-21, SafePatch Patch Server includes a list of all remote systems/hosts managed by SafePatch)

*which holds, for all computers to be managed by said software-property management* (e.g., page 2, section 1.1.1.2 Evaluating Remote Systems),

*information for identifying each computer* (e.g., page 34, host specification with OS type, name, version, and hardware type; page 28, section 4.2.1 Adding a Host to the Host List, i.e., from the list including all remote systems/hosts managed by SafePatch),

*are used as a basis on which a computer is extracted that is present in said network-connected-computer list and absent in said software-property management list* (e.g., pp. 28-29, creating/adding a brand new Host Group, which may

include remote systems/hosts currently connected with SafePatch but the Host Group is first time created/managed by SafePatch); *and*

*performing a second step wherein there is created a list of computer omitted in the software-property management based on the computer extracted that is present in said network- connected-computer list and absent in said software-property management list in the first step* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section 4.4, Scheduling a New Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management")

*wherein in the first step, said network-connected-computer list and said software-property management list are used as a basis on which a computer is extracted that is present in said software-property management list and absent in said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, wherein a SafePatch Agent software installed in a host is not running, i.e., present in a list of computers managed by SafePatch but not connectable;

page 49, section 7.3, host is Job List but unreachable, i.e., "absent in said network-connected-computer list" → said computer is extracted to trouble-shoot, pages 47 and 49, section 7.3), *and*

*in the second step, there is created a list of computer in unused state based on the computer extracted that is present in said software-property management list and absent in said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Claim 3:**

SafePatch discloses *a detection system for omission-in-software-property-management using a network for detecting a computer omitted from a software-property*

*management which manages, for each computer, basic information thereof and installed software, and fix-patch application status, comprising:*

*a network-connection management server including a network-connected-computer list* (e.g., Figure in page 31, list of alive remote systems/hosts after successfully testing their communications with Patch Server, page 30, section 4.3)

*which holds, for all computers connected to a given network, information for identifying each computer* (e.g., page 2, section 1.1.1.2 Evaluating Remote Systems; page 34, host specification with OS type, name, version, and hardware type)*;*

*a software-property management server including a software-property management list* (e.g., SafePatch overview, Figure in page 1 and pp. 17-21, SafePatch Patch Server includes a list of all remote systems/hosts managed by SafePatch)

*which holds, for all computers to be managed by said software-property management, information for identifying each computer; and an omission-in-software-property-management detection server* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section 4.4, Scheduling a New Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management")

*which uses said network-connected-computer list and said software-property management list as a basis to extract a computer that is present in said network-connected-computer list and absent in said software-property management list* (e.g., pp. 28-29, creating/adding a brand new Host Group, which may include remote systems/hosts currently connected with SafePatch but the Host Group is first time created/managed by SafePatch)*, and*

*to create a list of computer omitted in the software- property management based on the computer extracted that is present in said network-connected- computer list and absent in said software-property management list, wherein said omission-in-software-property-management detection server uses said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, wherein a SafePatch

Agent software installed in a host is not running, i.e., present in a list of computers managed by SafePatch but not connectable;

page 49, section 7.3, host is Job List but unreachable, i.e., "absent in said network-connected-computer list" → said computer is extracted to trouble-shoot, pages 47 and 49, section 7.3) *and*

*said software-property management list as a basis to extract a computer that is present in said software-property management list and absent in said network-connected-computer list, and to create a list of computer in unused state based on the computer extracted that is present in said software-property management list and absent in said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Claim 5:**

SafePatch discloses *the detection server for omission-in-software-property-management using a network for detecting a computer omitted from a software-property management which manages, for each computer, basic information thereof and installed software, and fix-patch application status,*

*wherein a network-connected-computer list* (e.g., Figure in page 31, list of alive remote systems/hosts after successfully testing their communications with Patch Server, page 30, section 4.3)

*which holds, for all computers connected to a given network, information for identifying each computer, is received from a network- connection-management server including said network-connected-computer list* (e.g., page 2, section 1.1.1.2 Evaluating Remote Systems; page 34, host specification with OS type, name, version, and hardware type),

*a software-property management list* (e.g., SafePatch overview, Figure in page 1 and pp. 17-21, SafePatch Patch Server includes a list of all remote systems/hosts managed by SafePatch)

*which holds, for all computers to be managed by said software-property management, information for identifying each computer, is received from a software-property management server including said software-property management list* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section 4.4, Scheduling a New Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management"), *and*

*said network-connected-computer list and said software-property management list are used as a basis on which a computer is extracted that is present in said network-connected- computer list and absent in said software-property management list* (e.g., pp. 28-29, creating/adding a brand new Host Group, which may include remote systems/hosts currently connected with SafePatch but the Host Group is first time created/managed by SafePatch), *and*

*there is created a list of computer omitted in the software-property management based on the computer extracted that is present in said network-connected-computer list and absent in said software-property management list* (e.g., pp. 30-31, section 4.3 Testing Communication, wherein a SafePatch Agent software installed in a host is not running, i.e., present in a list of computers managed by SafePatch but not connectable;

page 49, section 7.3, host is Job List but unreachable, i.e., "absent in said network-connected-computer list" → said computer is extracted to trouble-shoot, pages 47 and 49, section 7.3),

*wherein said server uses said network-connected-computer list and said software-property management list as a basis to extract a computer that is present in said software- property management list and absent in said network-connected-computer list, and to create a list of computer in unused state based on the computer extracted that is present in said software- property management list and absent in said*

*network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Claim 6:**

SafePatch discloses *a detection server for omission-in-software-property-management using a network for detecting a computer omitted from a software-property management which manages, for each computer, basic information thereof and installed software, and fix-patch application status, comprising:*

*a network-connection management section for creating a network-connected- computer list* (e.g., Figure in page 31, list of alive remote systems/hosts after successfully testing their communications with Patch Server, page 30, section 4.3)

*which holds, for all computers connected to a given network, information for identifying each computer; a software-property management section for creating a software-property management list* (e.g., SafePatch overview, Figure in page 1 and pp. 17-21, SafePatch Patch Server includes a list of all remote systems/hosts managed by SafePatch)

*which holds, for all computers to be managed by said software-property management, information for identifying each computer* (e.g., page 2, section 1.1.1.2 Evaluating Remote Systems; page 34, host specification with OS type, name, version, and hardware type)*; and*

*an omission-in-software-property-management detection section which uses said network-connected-computer list input from said network-connection management section* (e.g., pp. 28-29, creating/adding a brand new Host Group, which may include remote systems/hosts currently connected with SafePatch but the Host Group is first time created/managed by SafePatch)

*and said software-property management list input from said software-property management section as a basis to extract a computer that is present in said*

*network-connected-computer list and absent in said software-property management list* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section 4.4, Scheduling a New Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management"), *and*

*to create a list of computer omitted in software-property management wherein said omission-in-software-property-management detection section uses said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, wherein a SafePatch Agent software installed in a host is not running, i.e., present in a list of computers managed by SafePatch but not connectable;

page 49, section 7.3, host is Job List but unreachable, i.e., "absent in said network-connected-computer list" → said computer is extracted to trouble-shoot, pages 47 and 49, section 7.3) *and*

*said software-property management list as a basis to extract a computer that is present in said software-property management list and absent in said network-connected-computer list, and to create a list of computer in unused state* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Claim 9:**

SafePatch discloses *the detection server according to any of claims g4o-85 or 6, wherein said server sorts said network-connected-computer list and said software-property management list, and uses these sorted network-connected-computer list and software-property management list as a basis to create said list of a computer omitted in software-property management or-and said list of computer in unused state* (e.g., pp. 30-31, section 4.3 Testing Communication, wherein a SafePatch Agent software installed in a host is not running, i.e., present in a list of computers managed by SafePatch but not connectable; page 49, section 7.3, host is Job List but unreachable,

i.e., "absent in said network-connected-computer list" → said computer is extracted to trouble-shoot, pages 47 and 49, section 7.3).

**Claim 10:**

SafePatch discloses *a detection program, embedded in a computer-readable storage medium, for omission-in-software-property- management using a network for detecting a computer omitted from a software-property management which manages, for each computer, basic information thereof and installed software, and fix-patch application status,*

*wherein an omission-in-software-property-management detection server is allowed to receive a network-connected-computer list* (e.g., Figure in page 31, list of alive remote systems/hosts after successfully testing their communications with Patch Server, page 30, section 4.3)

*which holds, for all computers connected to a given network, information for identifying each computer, from a network- connection-management server including said network-connected-computer list* (e.g., page 2, section 1.1.1.2 Evaluating Remote Systems; page 34, host specification with OS type, name, version, and hardware type),

*receive a software-property management list* (e.g., SafePatch overview, Figure in page 1 and pp. 17-21, SafePatch Patch Server includes a list of all remote systems/hosts managed by SafePatch)

*which holds, for all computers to be managed by said software-property management, information for identifying each computer, from a software-property management server including said software-property management list* (e.g., pp. 28-29, creating/adding a brand new Host Group, which may include remote systems/hosts currently connected with SafePatch but the Host Group is first time created/managed by SafePatch), *and*

*use said network-connected-computer list and said software-property management list as a basis to extract a computer that is present in said network-connected- computer list and absent in said software-property management list* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section 4.4, Scheduling a New

Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management"), *and*

*to create a list of computer omitted in the software-property management based on the computer extracted that is present in said network-connected-computer list and absent in said software-property management list, wherein said omission-in-software-property-management detection server is allowed to use said network-connected-computer list and said software-property management list as a basis to extract a computer that is present in said software-property management list and absent in said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, wherein a SafePatch Agent software installed in a host is not running, i.e., present in a list of computers managed by SafePatch but not connectable;

page 49, section 7.3, host is Job List but unreachable, i.e., "absent in said network-connected-computer list" → said computer is extracted to trouble-shoot, pages 47 and 49, section 7.3), *and*

*to create a list of computer in unused state based on the computer extracted that is present in said software-property management list and absent in said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Claim 11:**

SafePatch discloses *a detection program, embedded in a computer-readable storage medium, for omission-in-software-property- management using a network for detecting a computer omitted from software-property management which manages, for each computer, basic information thereof and installed software, and fix-patch application status,*

*wherein an omission-in-software-property-management detection server is allowed to create a network-connected-computer list* (e.g., Figure in page 31, list of alive remote systems/hosts after successfully testing their communications with Patch Server, page 30, section 4.3)

*which holds, for all computers connected to a given network, information for identifying each computer, create a software-property management list* (e.g., SafePatch overview, Figure in page 1 and pp. 17-21, SafePatch Patch Server includes a list of all remote systems/hosts managed by SafePatch)

*which holds, for all computers to be managed by said software-property management, information for identifying each computer* (e.g., page 2, section 1.1.1.2 Evaluating Remote Systems; page 34, host specification with OS type, name, version, and hardware type), *and*

*use said network-connected-computer list and said software-property management list as a basis to extract a computer that is present in said network-connected- computer list and absent in said software-property management list* (e.g., pp. 28-29, creating/adding a brand new Host Group, which may include remote systems/hosts currently connected with SafePatch but the Host Group is first time created/managed by SafePatch), *and*

*to create a list of computer omitted in the software-property management based on the computer extracted that is present in said network-connected-computer list and absent in said software-property management list* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section 4.4, Scheduling a New Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management"),

*wherein said omission-in-software-property-management detection server is allowed to use said network-connected-computer list and said software-property management list as a basis to extract a computer that is present in said software-property management list and absent in said network-connected-computer list, and to create a list of computer in unused state based on the computer extracted that is*

*present in said software-property management list and absent in said network-connected-computer list* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Claim 13:**

SafePatch discloses *the detection program according to claim 10 or 11,*

*wherein an-said omission-in-software-property-management detection server is allowed to sort said network-connected-computer list and said software-property management list, and*

*to use these sorted network-connected-computer list and software-property management list as a basis to create said list of a computer omitted in software-property management or said list of computer in unused state* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Claim 14:**

SafePatch discloses *the detection method according to claim 1, wherein the network-connected-computer list is compared with the software-property management list as the basis on which the computer is extracted* (e.g., page 34, host specification with OS type, name, version, and hardware type; page 28, section 4.2.1 Adding a Host to the Host List, i.e., from the list including all remote systems/hosts managed by SafePatch).

**Claim 15:**

SafePatch discloses *the detection method according to claim 14, wherein the difference between the network-connected-computer list and the software-property management list is extracted* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section 4.4, Scheduling a New Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management").

**Claim 16:**

SafePatch discloses *the detection method according to claim 1, wherein the computer omitted in software-property management is a computer connected to the network not under software-property management* (e.g., pp. 30-31, section 4.3 Testing Communication, wherein a SafePatch Agent software installed in a host is not running, i.e., present in a list of computers managed by SafePatch but not connectable; page 49, section 7.3, host is Job List but unreachable, i.e., "absent in said network-connected-computer list" → said computer is extracted to trouble-shoot, pages 47 and 49, section 7.3).

**Claim 17:**

SafePatch discloses *the detection method according to claim 16, wherein the computer not under software-property management includes a computer operating under with an unknown operating system, software version, or patch-application status* (e.g., page 34, host specification with OS type, name, version, and hardware type; page 28, section 4.2.1 Adding a Host to the Host List, i.e., from the list including all remote systems/hosts managed by SafePatch).

**Claim 18:**

SafePatch discloses *the detection method according to claim 1, wherein the list of computer omitted in the software-property management includes information of the computer extracted* (e.g., pp. 28-29, after adding hosts/host group → pp. 31-32, section

4.4, Scheduling a New Job for said hosts/host group → page 33, section 4.5, Viewing a Report → pp. 39-40, details of report which creates a list of computer, such as Server 1 needing patch updates, i.e., a list of computer "omitted in software-property management").

**Claim 19:**

SafePatch discloses *the detection method according to claim 2, wherein the list of computer in unused state indicates a list of unused software* (e.g., pp. 30-31, section 4.3 Testing Communication, the host in a Job List but not "alive", i.e., unused/turned-off → page 4 paragraph 4., said computer in unused state is extracted to remotely trouble-shoot/turn-on, page 49, section 7.3; or said computer in unused state may be deleted from the Job List, page 28, section 4.2.1, paragraph 3.).

**Conclusion**

9. Any inquiry concerning this communication should be directed to examiner Thuy Dao (Twee), whose telephone/fax numbers are (571) 272 8570 and (571) 273 8570, respectively. The examiner can normally be reached on every Tuesday, Thursday, and Friday from 6:00AM to 6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Q. Dam, can be reached at (571) 272 3695.

The fax phone number for the organization where this application or proceeding is assigned is (571) 273 8300.

Any inquiry of a general nature of relating to the status of this application or proceeding should be directed to the TC 2100 Group receptionist whose telephone number is (571) 272 2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Thuy Dao/
Examiner, Art Unit 2192

/Tuan Q. Dam/
Supervisory Patent Examiner, Art Unit 2192